PHILADELPHIA FIRE DEPARTMENT **DIRECTIVE #57**
May, 2008

SUBJECT: FIRE DEPARTMENT WIDE AREA NETWORK

1. POLICY

This Directive addresses the policies, duties, responsibilities, and authority of the Office of Management Information Services and the Wide Area Network Administration, including all related issues concerning the PFD Wide Area Network and associated hardware and software.

2. DEFINITIONS

2.1 OFFICE OF MANAGEMENT INFORMATION SERVICES (MIS)

The Network Administrative Unit, located in Fire Headquarters, is responsible for the standardization, acquisition, maintenance and repair of the PFD Wide Area Network, and related equipment. Other responsibilities include furnishing guidance and advice to the Unit(s) involved in the development and maintenance of official PFD publications on the World Wide Web. The Network Administrative Unit is also charged with overseeing the PFD E-Mail System, as well as all aspects of Departmental Internet Access.

2.2 COMPUTER DOCUMENTATION

Instructional and Training aids have been developed by the Office of Management Information Services for use by all personnel. This documentation includes the PC Users Manual Booklet, the System Orientation presentation, as well as pertinent Chiefs' Staff Meeting Notes, Memoranda, E-Mail announcements, etc.

3. RESPONSIBILITY

It will be the responsibility of each member to exercise the appropriate control as directed by his/her rank in the implementation of this directive.

3.1 THE OFFICE OF MANAGEMENT INFORMATION SERVICES (MIS)

3.1.1 Exercise responsibility for the following:

a. evaluate and acquire approved hardware and software.

b. direct the installation of hardware, software and the evaluation of system malfunctions.

c. administer the repair and maintenance of all Wide Area Network computers and related equipment.

d. oversee the Network Administrative Unit.

e. approve all upgrades and modifications to the Network system in order to safeguard the integrity of the System.

3.2 NETWORK ADMINISTRATOR

3.2.1 Exercise responsibility for the following:

a. evaluation, acquisition, and deployment of Wide Area Network hardware and software.

b. determination of the optimal use for network resources-related hardware and software.

c. configuration, placement, and troubleshooting of all Wide Area Network computers, printers, and related hardware.

d. administer the distribution, configuration, and troubleshooting of all approved software and applications.

e. administration of electronic Inter-/Intra-Departmental communications (e-mail), including related hardware and software.

f. administration of all departmentally-sanctioned Internet Access Accounts.

g. maintenance and monitoring of Network Security, including Firewall, etc.

h. coordination of outside contractors and/or services relative to network functionality.

3.3 OFFICERS AND UNIT HEADS

3.3.1 Exercise responsibility for the following:

a. ensure that personnel using workstation computers do so in a manner that does not corrupt data, or damage hardware or software **- this includes prohibiting eating, drinking or smoking in the vicinity of workstations.**

b. **ensure that no unauthorized upgrades, changes, additions or repairs are made to the unit's computer, including both hardware and software.**

c. oversee the usage of the system and promptly report malfunctions to the Office of Management Information Services.

d. order, as needed, items such as disks, printer paper and printer toner cartridges from the warehouse and perform routine back-ups of the unit's local data.

3.4 USERS

It will be the responsibility of all members of the PFD to familiarize themselves and comply with the PFD Wide Area Network Directive and the PC User's Manual Booklet. **No one** is permitted to furnish their Log-in Password to any other personnel as this compromises Network and Unit security. Authorized users will adhere to the established city and departmental policies concerning e-mail and Internet usage. Users will make no unauthorized changes or modifications to departmental hardware or software. **Installation of unauthorized software is prohibited.**

3.5 E-MAIL USAGE GUIDELINES

3.5.1 Upon deployment and installation of Fire Department E-Mail software on a unit's workstation, users will familiarize themselves with the accompanying documentation (E-Mail Use Instructions and Lotus Notes Fundamentals).

3.5.2 E-mail communications should be drafted with the same care and formality as a printed or handwritten memorandum. They should not contain informal remarks that are potentially embarrassing or offensive to City personnel or to any other person. They should follow the same path, our chain-of-command, as printed memorandums. Carbon copying, (cc) someone above your immediate supervisor results in a breakdown of our chain-of-command. Issues that could be handled by the appropriate person, at the appropriate level, are not aware of the isssue if the chain-of-command is not used.

3.5.3 Use of City e-mail systems is subject to all applicable laws and city policies prohibiting infringement of intellectual property rights, harassment, discrimination, and defamation. You may not use e-mail for communications or transfers of information or data that:

a. infringe the copyright, trademark, or other intellectual property rights of third, parties (this includes communications and transfers that contain materials such as copyrighted materials, such as articles, books, photographs, and graphical images, in violation of copyright law); are otherwise illegal or wrongful or contrary to the established policies of the Fire Department or the City.

b. contain language that is defamatory, fraudulent, harassing, offensive, or discrimintory including, but not limited to, the display or transmission of sexually explicit images, cartoons, jokes, messages, chain letters, or other materials.

3.5.4 Privacy: The e-mail system and the messages sent and received on it are the property of the City. E-mail is received and stored on Fire Department and City network servers as well as individual desktop computers. The Office of Management Information Services and the Network Administrator reserve the right to access or disclose the stored e-mail messages and files of Fire Department employees in the course of carrying out their authorized duties. The Fire Department may monitor, review and disclose stored e-mail messages, without notice to the user, for various reasons. These include auditing purposes, to assure proper use of e-mail, to prevent security violations, to review job performance, or for any other reason deemed appropriate by the Fire Department. Although e-mail messages may be deleted from your desktop computer, they may continue to exist on network back-up or archival storage devices or on other systems beyond your control, and may be accessed even after you use the delete function. Users of the e-mail system, therefore, should not assume privacy or any right to privacy with respect to any e-mail communication to, from, or within the Fire Department or any other City agency.

In addition, e-mail and all other electronic communications, like paper documents, may be subject to the disclosure provisions of the Commonwealth of Pennsylvania’s Right to Know Act and/or the public records provisions of the Philadelphia Home Rule Charter. E-mail and all other electronic communications are subject to discovery during litigation and may be disclosed to or accessed by law enforcement authorities in the course of carrying out their official duties.

3.5.5 Records Retention: E-Mail communications are considered to be City property and may be retrieved from storage even though deleted by the sender and receiver.

E-Mail communications on City-owned equipment are public records and are the property of the Fire Department. They will be regulated by and managed with assistance from the Department of Records. There is no difference, for purposes of records retention and management, between paper record and documents, and electronic records and documents, including e-mail messages and attachments. If an e-mail communication and/or attachment falls within a record type identified in the Department's Record Retention Schedule, the e-mail must be saved for the period of time provided in the Schedule and deleted when that time has expired. Before deleting any e-mail message, users need to make a determination whether the message constitutes a public record under the Fire Department's Record Retention Schedule, and if it does, delete or retain the message in accordance with the requirements of the Schedule for records of similar type and content. Where retention is indicated, users may use the Lotus Notes Archiving function to save the record on their hard disk.

3.5.6 Members are advised that all existing Fire Department and City policies apply to your conduct on the e-mail system, especially (but not exclusively) those that deal with intellectual property protection, privacy, misuse of City resources, sexual and personal harassment, information and data security, and confidentiality. Failure to adhere to these policies may result in disciplinary action.

3.6 GUIDELINES FOR INTERNET USAGE

3.6.1 This section provides guidelines for appropriate and inappropriate use of the Internet by employees accessing the Internet from City premises and/or through City furnished computers, networks, or telecommunications facilities. Internet access is a resource provided by the city for employees to perform their city job responsibilities, and to enhance their ability to conduct the City's business. Internet use that is job-related fulfills these purposes and constitutes proper use; other use is prohibited.

3.6.2 The Office of Management Information Services and the Network Administrator reserve the right to monitor the Internet Usage of Department employees in the course of carrying out their authorized duties. The Fire Department may review and disclose monitored Internet pages without notice to the user, for auditing purposes, to assure proper use of Internet access, to prevent security violations, to review job performance, or for any other reason deemed appropriate by the Fire Department.

3.7 UNACCEPTABLE USES OF INTERNET ACCESS

3.7.1 Use of the Internet is subject to laws and City policies *prohibiting infringement of intellectual property rights, harassment, discrimination, and defamation*. As described below, you may not use your Internet access for communications or transfers of information or data that:

a. infringe the copyright, trademark, or other intellectual property rights of third parties (this includes communications and transfers that contain copy-righted materials, such as articles, books, photographs, and graphical images, in mages, in violation of copyright law).

b. are otherwise illegal or wrongful or contrary to the established policies of the Fire Department or the City.

c. contain language that is defamatory, fradulent, harassing, offensive, or discriminatory, including the display or transmission of sexually explicit images, cartoons, jokes, messages, or other materials (such activities are governed by the City of Philadelphia Fire Department Policy for Preventing Sexual Harassment in City Government, including Section C, relating to the Display of publications in City workplaces).

d. are personal in nature.

e. support a private business enterprise.

f. are inconsistent with the performance of one's assigned duties.

3.7.2 Confidential or sensitive city information may not be distributed over or in any way posted on the Internet. Transmission and distribution of Fire Department information for city business purposes is subject to the rules and policies of each unit, as well as the Fire Department.

3.7.3 All use of the Internet for e-mail communication is subject to the city's current Electronic Mail Policy, including, but not limited to, the following rules:

a. Internet e-mail messages can be intercepted by third parties and should not contain City information that is confidential, sensitive, or otherwise unsuitable for distribution to the public.

b. **You may not send or receive e-mail messages under a user name, account number, or other identifying information other than the account provided to you by the City.**

c. You may not use city furnished Internet access or Fire Department computers, networks, or telecommunications facilities to send personal e-mail messages (i.e., e-mail messages that are not directly related to the conduct of City business) over the Internet.

3.7.4 In accordance with City policy requiring that City facilities be used only for City business, you may not use your City furnished Internet access or City furnished computers, networks, or telecommunications facilities to:

a. promote political candidates or otherwise engage in political activity.

b. participate in public debate on the Internet (including but not limited to "chat rooms" and bulletin boards) unless it is directly related to your job duties and has the approval of your supervisor.

c. participate in public debate or information exchanges in a way that suggests your personal views are official views or policies of the City.

3.7.5 You are not permitted to access the Internet from Fire Department premises and/or through City furnished computers, networks, or telecommunications facilities for personal use (i.e., use for any purpose not directly related to the conduct of City business).

3.7.6 **You may not use City equipment to access your personal (i.e., not City provided) Internet account, Internet service provider, or other on-line service.**

3.7.7 You may not use City computers or City-furnished Internet access to create, host, or maintain personal Internet pages.

3.7.8 **You may not use any user name or network password but your own** to access the Internet without the knowledge and express consent of the person to whom they are assigned, except as authorized by your supervisor.

3.8 ACCEPTABLE USES OF INTERNET ACCESS

3.8.1 Some general examples of acceptable use include, with the approval of one's unit head, the following:

a. searching the Internet for information relating to a current project required by your assigned job duties.

b. searching for and downloading information for purposes of job-related training for yourself or for others.

c. sending and receiving e-mail messages to non-City personnel in the course of conducting Department business (such as contractors and consultants), provided that the messages do not contain confidential or sensitive City information.

d. exchanging information with officials and employees of other governments on topics related to your job functions.

3.9 THE FIREWALL

Access to and from the Internet through City Net is protected by a “firewall” which is a specialized computer and software that prevents Internet users from gaining access to City computers and data unless they are authorized to do so. Any PC linked to City Net that is connected to the Internet directly (e.g., via modem and telephone lines) and not through the firewall creates a serious and unacceptable security risk for City computers and data. City and Fire Department policy strictly prohibits the connection of any such “networked” PC with the Internet except through the firewall.

3.10 ADMINISTRATION OF ACCESS

Access to the Internet for computers linked to City Net is administered jointly by the Mayor’s Office of Information Services (MOIS) and the Department of Public Property, Communications Division, as well as the Fire Department’s Office of Management Information Services and Network Administrative Unit. Access will be granted only to the extent that a clear business and technical requirement is established by the requesting unit. The unit’s account will reflect usage, including the Internet sites visited and the time logged onto the Internet. A summary of each account, similar to current summaries of long distance telephone use, will be available to the Fire Department from MOIS and the Communications Division.

4. GENERAL INFORMATION

4.1 No one is to release computerized data to any outside agency without the approval of the Fire Commissioner.

4.2 All computers, related hardware, and software will be issued by the Office of Management Information Services, which is solely responsible for all administrative aspects, logistics of deployment, and use of said equipment.

4.3 All computers, related hardware, and software in Fire Department installations are subject at any time to inspection by the Office of Management Information Services.

4.4 Any conflicts stemming from a unit’s deviation from the aforementioned policies are subject to the review of, and resolution by, the Commissioner and the Deputy Commissioner for Administrative Services.

4.5 Only the Office of Management Information Service's personnel are authorized to order vendor repairs on Fire Department computers.

4.6 When a computer fails to operate properly, the commanding officer will immediately contact the Office of Management Information Services, providing such information as the computer's public property number, serial number, text of error messages, and computer activity immediately preceding problem, etc.

BY ORDER OF THE FIRE COMMISSIONER